Chapter 3 Composite Risk Management (CRM)

3-1. General

- a. CRM is a leadership responsibility. Commanders/supervisors at every level will employ CRM to effectively control safety and occupational health risks to missions, personnel, equipment, and the environment.
- b. CRM is the best process for protecting the force. It is a tool to help leaders make sound decisions in a systematic, logical thought process to identify and control hazards. Through integration, leaders and individuals are empowered with the responsibility, authority, and accountability for CRM decisions at the most appropriate level.

3-2. Responsibilities

- a. CRM is our most effective tool to protect the force by providing a systematic framework for identifying and controlling risks in all environments. Commanders will accept no risk unless the potential benefit outweighs the potential loss. The level of risk determines which commanders are responsible.
- (1) *Extremely high risk* CASCOM Commander, Commandants of Quartermaster, Ordnance or Transportation Schools, and DeCA Commander.
- (2) *High risk* Colonels, Commanders, Commandants or heads of separate organizations, or equivalent in the appropriate chain of command.
- (3) *Moderate risk* Lieutenant Colonels, Battalion Commanders/Department Directors, or equivalent in the appropriate chain of command.
- (4) Low risk Company Commanders, Division Chiefs, or equivalent in the appropriate chain of command.
- b. All risk decisions will be based on the residual risk of an activity after applying appropriate control measures. However, CRM does not eliminate risk or the necessity for standards and will not be used to sanction or justify violating the law.

c. Commanders/directors will:

- (1) Establish risk approval procedures within their organization ensuring that risk assessments for high risk and extremely high risk training and operations on the installation are forwarded to the Senior Commander or the Commandants of Quartermaster, Ordnance or Transportation Schools as appropriate.
- (2) Complete written risk assessments of all training and operations for inherent risk or hazards using DA Form 7566, Composite Risk Management Work Sheet, which is located at the back of this regulation.
 - (3) Ensure countermeasures are developed and implemented to reduce risk.

- (4) Ensure that risk assessments are reviewed prior to the start of training and operations to ensure conditions have not changed and to ensure that effective countermeasures are adhered to throughout the training and operation.
 - (5) Ensure personnel are trained and understand the CRM process as needed.
- (6) Establish alternate risk approval procedures within deployable units for use when training and operations are conducted away from the installation.
 - d. The Installation Safety Office will:
- (1) Provide technical assistance in analysis and preparation of risk assessments as needed for low and medium risk.
- (2) Review and analyze risk assessments for all high risk operations and training and make recommendations to commanders/supervisors to reduce risk.
- (3) Provide training support for CRM as needed. Refer personnel to the U.S. Amy Combat Readiness/Safety Center (CRC) website at appendix A, section III, in the back of this regulation.
- (4) Provide on-site training or operations inspections to ensure compliance with this regulation. Report findings to commander or director.
 - e. Supervisors will:
 - (1) Assess all training and operations for inherent risk or hazards.
 - (2) Conduct job hazard analysis in conjunction with employee.
- (3) Complete written risk assessment prior to conducting training and operations for inherent risk or hazards.
 - (4) Train subordinates in CRM principles and techniques.

3-3. Composite Risk Management principles

Risk is the potential severity of a loss combined with the probability of an occurrence. The loss can be death, injury, property damage, or mission failure. CRM identifies risks associated with a particular operation and weighs those risks against the overall value to be gained. The four principles of CRM are:

- a. Accept no unnecessary risk.
- b. Accept risks when benefits outweigh costs.
- c. Make risk decisions at the proper level consistent with command policy.
- d. Manage risk in the concept and planning stages whenever possible.

3-4. Composite Risk Management process

The CRM process involves identifying and controlling hazards. The five steps represent a logical thought process from which users develop tools, techniques, and procedures for applying CRM in their areas of responsibility. It is a closed loop process applicable to any situation and environment.

- a. *Step 1*. Identify hazards to the force or mission. Consider all aspects of current and future situations, environment, and known historical problems.
- b. *Step 2*. Assess the risk to determine risk decisions. Develop the impact of each hazard in terms of potential loss and cost based on probability and severity. Ask these questions:
 - (1) What type of injury or equipment damage can be expected?
- (2) What is the probability of an accident happening? An expected minor injury combined with an unlikely probability equals low risk. An expected fatality combined with a frequent probability equals extremely high risk.
- c. Step 3. Develop controls and make risk decisions. If you cannot eliminate the risk, you must control it without sacrificing essential mission values. Some risks can be controlled by modifying tasks, changing location or route, increasing supervision, wearing protective clothing, changing time of operation, etc. A leader must usually decide between selecting from available controls, stopping the mission because the risk is too great, or accepting risk because mission benefits outweigh potential loss.
- d. *Step 4*. Implement control measures. Put controls in place that eliminate the hazards or reduce their risks. Integrate procedures to control risks into plans, orders, SOPs, lesson plans, etc. Also ensure risk reduction measures are used during actual operations.
- e. *Step 5*. Supervise and evaluate. Enforce standards and controls, then evaluate the effectiveness of controls and adjust/update as needed. Make sure leaders know what controls are in place and what standards are expected, then hold those in charge accountable for implementation from start to finish. This is where accident prevention actually occurs.

3-5. Risk assessment

The Army uses two similar hazard assessment matrices.

- a. The following risk assessment matrix from AR 385-10 is used when a hazard is identified in a normal workplace that could be covered under the Occupational Safety and Health Act standards (table 3-1).
 - b. A risk assessment matrix from Army doctrine used for operational hazards is at table 3-2.

Risk Assessment Matrix

E=	E = Extremely High Risk		PROBABILITY					
H = High Risk		Frequent	Likely	Occasional	Seldom	Unlikely		
	M = Moderate RiskL = Low Risk		A	В	С	D	E	
SEVERITY	CATASTROPHIC	I	Ε	Ш	Н	Ι	M	
	CRITICAL	II	E	I	Н	M	L	
	MARGINAL	III	H	M	M	٦	L	
	NEGLIGIBLE	IV	M	L	L	L	L	

Table 3-1. Risk Assessment Matrix

PROBABILITY							
Frequent	Likely	Occasional	Seldom	Unlikely			

Frequent – Occurs very often, known to happen regularly.

Likely – Occurs several times, a common occurrence.

Occasional – Occurs sporadically, but is not uncommon.

Seldom – Remotely possible, could occur at some time.

Unlikely – Can assume it will not occur, but not impossible.

SEVERITY						
Catastrophic	Ι	Complete mission failure or the loss of ability to accomplish a mission. Death or permanent total disability. Loss of major or mission-critical systems or equipment. Major property or facility damage. Severe environmental damage. Mission-critical security failure. Unacceptable collateral damage.				
Critical	II	Severely degraded mission capability or unit readiness. Permanent partial disability or temporary total disability exceeding three months time. Extensive major damage to equipment or systems. Significant damage to property or the environment. Security failure. Significant collateral damage.				
Marginal	III	Degraded mission capability or unit readiness. Minor damage to equipment or systems, property, or the environment. Lost days due to injury or illness not exceeding three months. Minor damage to property or the environment.				
Negligible	IV	Little or no adverse impact on mission capability. First aid or minor medical treatment. Slight equipment or system damage, but fully functional or serviceable. Little or no property or environmental damage.				

Table 3-2. Risk assessment probability